# NASA Counterintelligence Note

**Office of Protective Services | Counterintelligence/Counterterrorism Division**
**300 E Street SW, Suite CU78**
**Washington, DC 20546, 202-358-3198**

## INSIDER THREATS: Six Types of Employees who can Wreak Havoc in Your Organization

This Counterintelligence (CI) Note provides situational awareness regarding employee personalities that may pose a threat to their organizations. This information is taken entirely from an article posted on www.nextgov.com and was written by Brian White who serves as the chief operating officer of RedOwl, a "next-generation security analytics firm focused on both compliance and insider threats."

**BACKGROUND:**

Leonard Glenn Francis (aka "Fat Leonard") is the **"man who seduced the Seventh Fleet**." For years, the Singapore-based businessman showered Navy officers with gifts, fed them magnificent dinners, procured escorts for them, and gave them cash bribes. His goal: gain intelligence about US Navy operations so he could cheat the Navy on contracts to refuel and resupply its ships.

It has been called the worst national security breach in the Navy since the Cold War. In return for his largesse, Fat Leonard had access to classified information about U.S. warship and submarine movements – information that, had he been minded to, would have been of great value to China.

Fat Leonard also got confidential contracting information and files about active law enforcement investigations into his company. To date, 14 naval officers have been arrested and charged with crimes, **including three just last month**.

Fat Leonard himself was lured to the U.S., arrested in a sting operation, and has pleaded guilty. He is cooperating with the government and awaits sentencing.

How could this happen? How could so many Navy officers be compromised? And of even greater importance, how could the Navy be unaware? The failure is a cautionary tale about how *not* to approach the problem of insider threats.

The problem is not just confined the Navy. Recently, John Carlin, assistant attorney general for national security, **noted**:

"We still do the traditional spy cases. But **a lot of the cases now are not traditional espionage**, insofar as they're not necessarily a trained member of the other country's spy service. Instead, **they're getting the information by cyber-enabled means or stealing it by bribing an insider**."

The insider threat is not just a cybersecurity problem or a data analytics issue; it's a human risk problem that can only be solved by understanding how people think and behave. There are certain signals that, with context, can pinpoint an insider threat before they strike. For example, the Fat Leonard case can be identified with one type of threat -- the bribed insider.

Here is how we would describe this threat: This "Type A" employee quickly made captain (or vice president in a private sector company) and reached a senior, well-respected position across the enterprise. One day at a conference, he was approached by an individual (in this case Fat Leonard) from another country, who struck up a conversation. They began socializing on a fairly regular basis.

With your employee's help, this foreigner got inside information about the enterprises operations and plans. The employee's activities are reflected in frequent communications with external contacts, clear monetary motivation and a willingness to skirt the rules to get ahead.

The realm of the insider risk is broad, reaching beyond the classic bribed insider example. Consider the following five additional personas of individuals who represent insider threat risks within companies and organizations:

**The Saboteur**

This employee may be introverted and extremely detail oriented. They may feel underappreciated and overlooked by management, causing them to become frustrated and careless about their work. You might notice them openly searching for a new job during work hours.

As a result, they may have a huge fight with their boss and quit, leaving a "time bomb" program that will go off months after their departure, wiping important HR records.

**The Intellectual Property Thief**

Focused on climbing the corporate ladder, this leader has little time for those beneath their position, yet typically feels undervalued. They're often calculated when they resign, planning to go to a key competitor, taking valuable intellectual property with them.

Unfortunately, these employees are often senior team members with a high level of access to sensitive information like client information, studies, strategies and business plans.

**The Entitled Individual**

This is your heavy hitter. They've been with your company for years, have significantly grown the business, and are primarily motivated by money -- and little else.

Courted by your biggest rival with a sweet deal, she wipes her work devices. She feels like she deserves it after years of work, taking your client roster, product ideas, pitch materials and more. She'll spend the weeks before her departure gathering as much information as she can take.

**The Blackmailed Contractor**

Your contractor may be targeted by an organized crime network because of his technical position of trust on LinkedIn. The blackmailer may pose as a technical recruiter and convince him to steal sensitive personally identifiable information that can be sold through the black market.

After he finds vulnerable information to exploit, he will become more confident and aggressive about stealing this information. Eventually, he will become sloppy and prepares his resignation to avoid being caught.

**The Media Leaker**

This insider will become privy to some internal communications of corporate executives about compensation. Chats and emails about helicopter rides and extravagant dinners on the company dime, whether to fire mid-level managers who didn't seem smart enough, and even disparaging and sexist remarks about a female admin assistant.

This employee gets frustrated and decides she's had enough. She shifts her hours so she can surreptitiously document these conversations over a period of weeks or months. When she is ready to quit, she takes her dirt and sends it straight to her friend at a national media publication.

Any one of these employees could seriously damage your organization. The recent **Verizon Data Breach Investigations Report** revealed **77 percent of breaches were a result of insiders and notes that insider risks are some of the hardest to detect**, as seen in the Fat Leonard case.

Understanding behaviors and human nature is the only way to truly help organizations understand when and insider could transform from an ally to an enemy. Keeping an eye out for the above personas that exemplify insider risk is the best place to start.

**Reporting Suspected Insider Threat Activity:**

If you have concerns about anyone who may pose a threat to NASA people, information, technology, facilities, etc., please contact your servicing security office or Counterintelligence Special Agent. A link to the points of contacts for all the Agency's Counterintelligence/Counterterrorism offices is below:

http://www.hq.nasa.gov/office/ops/nasaonly/internal/ci/poc.htm

Link to original article:

http://www.nextgov.com/technology-news/tech-insider/2016/07/6-employees-who-could-wreak-havoc-your-organization/130152/?oref=ng-HPriver&

This NASA Counterintelligence Note was prepared by Regional Counterintelligence Director Arthur R. Payton.
arthur.r.payton@nasa.gov
(202) 358-4645